Applying User Sessions to Detect SQL Injection Vulnerabilities in Web Applications

Isaiah Yoon Mengni Du **Sreedevi Sampath**
University of Maryland Baltimore County
UMBC
AN HONORS UNIVERSITY IN MARYLAND
http://www.umbc.edu/~sampath
sampath@umbc.edu

SQL Injection and User Sessions

- SQL Injection Vulnerability topped the 2011 MITRE Common Weakness Enumeration (CWE)/SANS Top 25 Most Dangerous Software Errors list
- Clickstream data is an invaluable source to detect previously unknown SQL Injection vulnerabilities
- User sessions are test cases created from clickstream data

The Larger Project View

- **Goal**: Identify SQL Injection Vulnerabilities in web applications
- **Problem**: Difficult to generate test cases targeted to find such faults
- **Solution**: Reduce and modify user sessions to create test cases capable of exposing SQL Injection vulnerabilities in web applications

User-Session-Based Testing

- **Test Suite**: set of test cases
- **Test Case**: sequence of URLs + name-value pairs

Example:
http://schoolmate/login.php?login=john&pass=mypass

Challenge: Create a framework to automatically find SQL Injection vulnerabilities in web applications

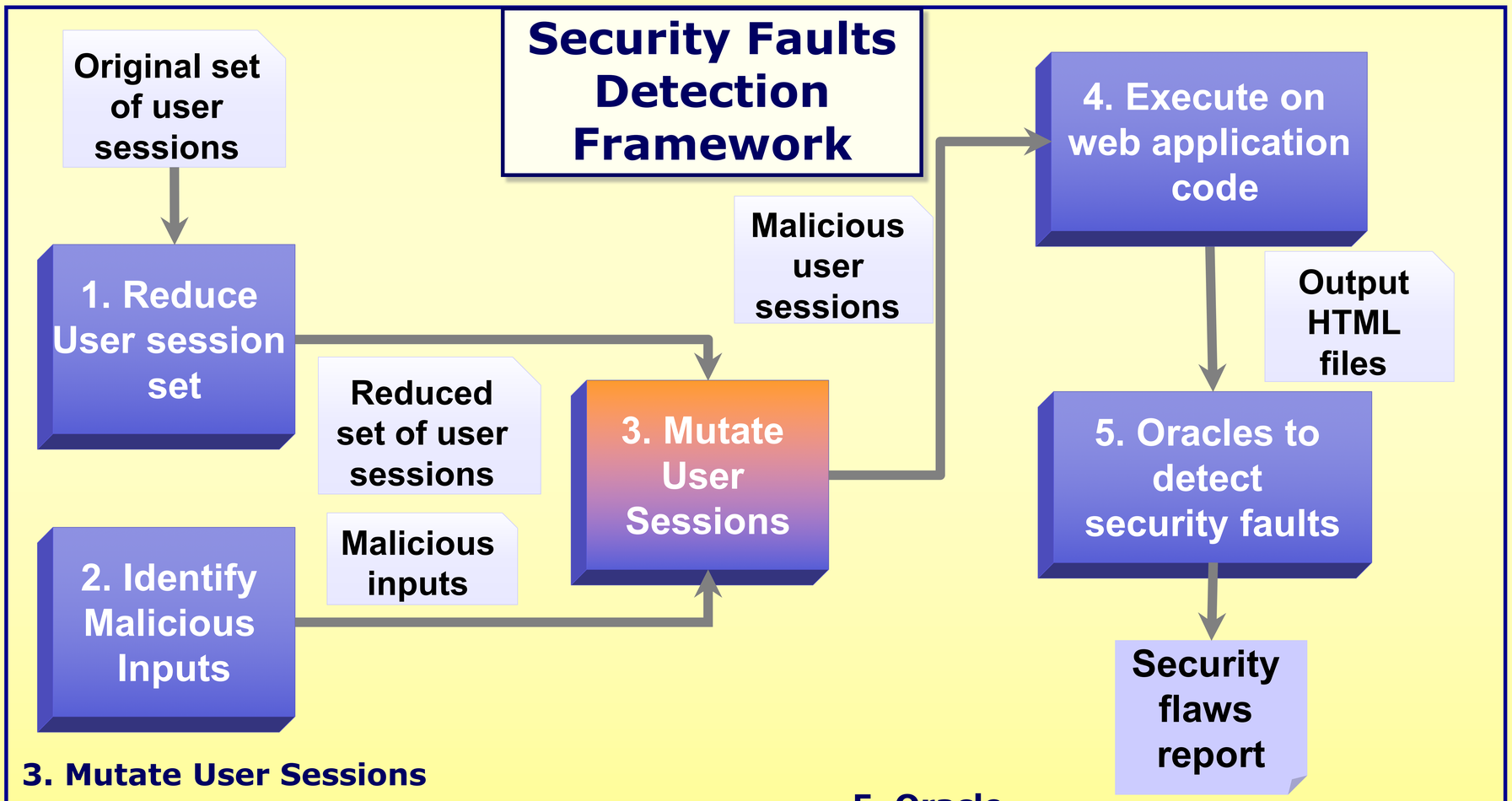
1. Reduce User Session Set

- Applied popular reduction algorithm, HGS, with two requirements
  - base URL (login.php)
  - URL-name (login.php-login,pass)
- **Goal:** Find a reduced set of test cases that has all base URLs/URL-names that exist in original suite

Requirement	No. Test Cases	Percent Reduction
Original	125	
Base URL	9	92.8%
URL-name	47	62.4%

2. Identify Malicious Inputs

- Web search for example values used in SQL Injection Attacks
- Blind, Error-based, Time delay, Union exploitation, Stacked-query
- We identified 114 malicious inputs



3. Mutate User Sessions

- Identify vulnerable parameters used in SQL queries in code
- Replace values of vulnerable parameters in user sessions with malicious inputs
- New malicious user sessions:
  Base URL: 1026, **URL name:** 5358

5. Oracle

- Run malicious and clean test cases on web application
- Intelligent Diff of output
- Output differs → user session detected fault